REMARKS

In response to the Notice of Panel Decision dated July 20, 2009, and in further response to the Office Action dated December 24, 2008, Applicants respectfully request reconsideration and withdrawal of the rejections of the claims.

Claims 1-6 and 8-18 were rejected under 35 USC 103 on the basis of the Futa et al patent in view of the Hopkins et al patent. Claim 7 was rejected under 35 USC 103 on the basis of these two patents, in further view of the Matyas patent. It is respectfully submitted that the Futa and Hopkins patents do not teach all of the elements of the rejected claims, and therefore any logical combination of their teachings would not result in the claimed subject matter. Accordingly, Applicants traverse the basis upon which the rejection is founded.

To expedite the examination of the application, and reduce the issues under consideration, the subject matter of claim 11 has been incorporated into claim 1. To further distinguish the invention from the prior art represented by the Futa and Hopkins patents, new claim 19 has been added. For the reasons presented hereinafter, it is respectfully submitted that all pending claims are patentably distinct from the references of record.

Claim 1, as amended. recites a method of generating keys for public-key cryptography. A first calculation step of the method comprises calculating pairs of prime numbers independent of the values for e (a public exponent) and l (length of the key of the cryptography method), and storing the resulting pairs. As a second step, one of the pairs is evaluated to verify whether it meets two conditions, namely whether (i) the two numbers of the pair are prime with respect to a given value for e, and (ii) the product of the pair of numbers has a length equal to l. If the selected pair

of prime numbers does not meet these conditions, a new pair of prime numbers is selected, and the procedure is repeated. Once a pair of prime numbers is found that meets these conditions, a key d is calculated on the basis of these two prime numbers.

In rejecting claim 11, whose subject matter is now incorporated into claim 1, the Office Action acknowledges that the Futa patent does not disclose the repeated verification of two selected prime numbers against the conditions recited in the claim until a pair of prime numbers is found that meets the conditions. To this end, therefore, it asserts that such features are disclosed in the Hopkins patent, and that it would be obvious to modify the technique of the Futa patent in light of such disclosure. It is respectfully submitted that the Hopkins patent does not disclose the claimed features that are alleged in the Office Action.

More particularly, at paragraphs 0057 and 0058, cited in the Office Action, the Hopkins patent discloses that a plurality of k (where k is greater than 2) prime numbers are developed, and each is checked to ensure that a derivative of that number, i.e. p_n-1, is relatively prime to e. The Hopkins patent does not disclose that the product of two of these numbers is evaluated to determine whether its length is equal to a given value I. Rather, it discloses that the composite number n, which is the product of *more than 2* of the prime numbers, "provides" a modulus for encoding and decoding operations (paragraph 0058, lines 1-2). In other words, the composite number dictates the length of the key, rather than being tested to determine whether it has the same length as a given value I.

Consequently, the Hopkins patent does not disclose that a *pair* of selected prime numbers is evaluated to verify whether it meets both of the conditions recited

in claim 1, as amended. As such, any reasonable application of the teachings of the Hopkins patent to the procedure of the Futa patent would not lead a person of ordinary skill in the art to the subject matter of claim 1.

For similar reasons, the Hopkins patent does not disclose the subject matter of claim 12 that was acknowledged to be absent from the Futa patent, namely a communication means for receiving at least one pair of values (e, I). Since the encryption/decryption modulus is provided by the composite number n, the system of the Hopkins patent does not "receive" a value for the length of the modulus from some external source. Nor is there any reason to include a communication means for receiving such a value, since the system itself calculates the composite number the determines the modulus.

Accordingly, it is respectfully submitted that the Hopkins patent does not disclose those features of claims 1 and 12 that are acknowledged in the Office Action to be missing from the Futa patent. Any reasonable combination of the two references would therefore not result in the subject matter recited in these two claims.

New claim 19 recites a further distinguishing feature of the invention, namely that the calculation of the pairs of prime numbers takes place on a computing resource, such as a server, that is external to the electronic device that uses a key for a cryptographic algorithm, e.g. a chip card. After the prime numbers have been calculated, they are stored on the electronic device, and then the device calculates a key for the algorithm, by first testing a stored pair of the prime numbers to verify whether it meets to conditions, and then using a pair of prime numbers that meets these conditions to generate the key. Support for this claimed subject matter can be

found, for example, at page 13, lines 7-12 and 20-26 of the specification. In contrast, the Futa patent discloses that all operations take place on the memory card 10.

It is respectfully submitted that independent claims 1, 12 and 19 are patentably distinct from the prior art of record. Dependent claims 2-10 and 13-18 are submitted to be likewise patentable for at least these same reasons. Reconsideration and withdrawal of the rejections are therefore respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date:3 November 20, 2009

By: /James A. LaBarre/
James A. LaBarre
Registration No. 28632

Customer No. 21839
703 836 6620